BLOCKCHAIN BASICS

A NON-TECHNICAL INTRODUCTION IN 25 STEPS

Daniel Drescher

Apress®

Blockchain Basics: A Non-Technical Introduction in 25 Steps

Daniel Drescher
Frankfurt am Main, Germany

ISBN-13 (pbk): 978-1-4842-2603-2 ISBN-13 (electronic): 978-1-4842-2604-9
DOI 10.1007/978-1-4842-2604-9

Library of Congress Control Number: 2017936232

Managing Director: Welmoed Spahr
Editorial Director: Todd Green
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Technical Reviewer: Laurence Kirk
Coordinating Editor: Rita Fernando
Copy Editor: Mary Bearden
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484226032. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Apress Business: The Unbiased Source of Business Information

Apress business books provide essential information and practical advice, each written for practitioners by recognized experts. Busy managers and professionals in all areas of the business world—and at all levels of technical sophistication—look to our books for the actionable ideas and tools they need to solve problems, update and enhance their professional skills, make their work lives easier, and capitalize on opportunity.

Whatever the topic on the business spectrum—entrepreneurship, finance, sales, marketing, management, regulation, information technology, among others—Apress has been praised for providing the objective information and unbiased advice you need to excel in your daily work life. Our authors have no axes to grind; they understand they have one job only—to deliver up-to-date, accurate information simply, concisely, and with deep insight that addresses the real needs of our readers.

It is increasingly hard to find information—whether in the news media, on the Internet, and now all too often in books—that is even-handed and has your best interests at heart. We therefore hope that you enjoy this book, which has been carefully crafted to meet our standards of quality and unbiased coverage.

We are always interested in your feedback or ideas for new titles. Perhaps you'd even like to write a book yourself. Whatever the case, reach out to us at editorial@apress.com and an editor will respond swiftly. Incidentally, at the back of this book, you will find a list of useful related titles. Please visit us at www.apress.com to sign up for newsletters and discounts on future purchases.

The Apress Business Team

Contents

About the Author

Daniel Drescher is an experienced banking professional who has held positions in electronic security trading in several banks. His recent activities have focused on automation, machine learning, and big data in the context of security trading. Among others, Daniel holds a doctorate in econometrics from the Technical University of Berlin and an MSc in software engineering from the University of Oxford.

About the Technical Reviewer

Laurence Kirk who after a successful career writing low latency financial applications for the City of London, was captivated by the potential of distributed ledger technology. He moved to Oxford to study for his master's degree and set up Extropy.io, a consultancy working with start-ups to develop applications on the Ethereum platform. Passionate about distributed technology, he now works as a developer, evangelist, and educator about Ethereum.

Introduction

This introduction answers the most important question that every author has to answer: Why should anyone read this book? Or more specifically: Why should anyone read another book about the blockchain? Continue reading and you will learn why this book was written, what you can expect from this book, what you cannot expect from this book, for whom the book was written, and how the book is structured.

Why Another Book About the Blockchain?

The blockchain has received a lot of attention in the public discussion and in the media. Some enthusiasts claim that the blockchain is the biggest invention since the emergence of the Internet. Hence, a lot of books and articles have been written in the past few years about the blockchain. However, if you want to learn more about how the blockchain works, you may find yourself lost in a universe of books that either quickly skim over the technical details or that discuss the underlying technical concepts at a highly formal level. The former may leave you unsatisfied because they miss to explain the technical details necessary to understand and appreciate the blockchain, while the latter may leave you unsatisfied because they already require the knowledge you want to acquire.

This book fills the gap that exists between purely technical books about the blockchain, on the one hand, and the literature that is mostly concerned with specific applications or discussions about its expected economic impact or visions about its future, on the other hand.

This book was written because a conceptual understanding of the technical foundations of the blockchain is necessary in order to understand specific blockchain applications, evaluate business cases of blockchain startups, or follow the discussion about its expected economic impacts. Without an appreciation of the underlying concepts, it will be impossible to assess the value or the potential impact of the blockchain in general or understand the added value of specific blockchain applications. This book focuses on the underlying concepts of the blockchain since a lack of understanding of a new technology can lead to being carried away with the hype and being disappointed later on because of unrealistic unsubstantiated expectations.

This book teaches the concepts that make up the blockchain in a nontechnical fashion and in a concise and comprehensible way. It addresses the three big questions that arise when being introduced to a new technology: What is it? Why do we need it? How does it work?

What You Cannot Expect from This Book

The book is deliberately agnostic to the application of the blockchain. While cryptocurrencies in general and Bitcoin in particular are prominent applications of the blockchain, this book explains the blockchain as a general technology. This approach has been chosen in order to highlight generic concepts and technical patterns of the blockchain instead of focusing on a specific and narrow application case. Hence, this book is:

- Not a text specifically about Bitcoin or any other cryptocurrency
- Not a text solely about one specific blockchain application
- Not a text about proofing the mathematical foundations of the blockchain
- Not a text about programming a blockchain
- Not a text about the legal consequences and implications of the blockchain
- Not a text about the social, economic, or ethical impacts of the blockchain on our society or humankind in general

However, some of these points are addressed to some extent at appropriate points in this book.

What You Can Expect from This Book

This book explains the technical concepts of the blockchain such as transactions, hash values, cryptography, data structures, peer-to-peer systems, distributed systems, system integrity, and distributed consensus in a nontechnical fashion. The didactical approach of this book is based on four elements:

- Conversational style
- No mathematics and no formulas
- Incremental steps through the problem domain
- Use of metaphors and analogies

Conversational Style

This book is deliberately written in a conversational style. It does not use mathematical or computer science jargon in order to avoid any hurdle for nontechnical readers. However, the book introduces and explains the necessary terminology needed to join the discussion and to understand other publications about the blockchain.

No Mathematics and No Formulas

Major elements of the blockchain such as cryptography and algorithms are based on complex mathematical concepts, which in turn come with their own demanding and sometimes frightening mathematical notation and formulas. However, this book deliberately does not use any mathematical notation or formulas in order to avoid any unnecessary complexity or hurdle for nontechnical readers.

Incremental Steps Through the Problem Domain

The chapters in this book are called *steps* for a good reason. These steps form a learning path that incrementally builds the knowledge about the blockchain. The order of the steps was chosen carefully. They cover the fundamentals of software engineering, explain the terminology, point out the reason why the blockchain is needed, and explain the individual concepts that make up the blockchain as well as their interactions. Calling the individual chapters steps highlights their dependence and their didactical purpose. They form a logical sequence to be followed instead of being chapters that could be read independently.

Use of Metaphors and Analogies

Each step that introduces a new concept starts with a pictorial explanation by referring to a situation from real life. These metaphors serve four major purposes. First, they prepare the reader for introduction to a new technical concept. Second, by connecting a technical concept to an easy-to-understand real-world scenario, the metaphors reduce the mental hurdle to discover a new territory. Third, metaphors allow learning new concepts by similarities and analogies. Finally, metaphors provide rules of thumb for memorizing new concepts.

How This Book Is Organized

This book consists of 25 steps grouped into five major stages that all together form a learning path, which incrementally builds your knowledge of the blockchain. These steps cover some fundamentals of software engineering, explain the required terminology, point out the reasons why the blockchain is needed, explain the individual concepts that make up the blockchain as well as their interactions, consider applications of the blockchain, and mention areas of active development and research.

Stage I: Terminology and Technical Foundations

Steps 1 to 3 explain major concepts of software engineering and set the terminology necessary for understanding the succeeding steps. By the end of Step 3, you will have gained an overview of the fundamental concepts and an appreciation of the big picture in which the blockchain is located.

Stage II: Why the Blockchain Is Needed

Steps 4 to 7 explain why the blockchain is needed, what problem it solves, why solving this problem is important, and what potential the blockchain has. By the end of Step 7, you will have gained a good understanding of the problem domain in which the blockchain is located, the environment in which it provides the most value, and why it is needed in the first place.

Stage III: How the Blockchain Works

The third stage is the centerpiece of this book since it explains how the blockchain works internally. Steps 8 to 21 guide you through 15 distinct technical concepts that all together make up the blockchain. By the end of Step 21, you will have reached an understanding of all the major concepts of the blockchain, how they work in isolation, and how they interact in order to create the big machinery that is called the blockchain.

Stage IV: Limitations and How to Overcome Them

Steps 22 to 23 focus on major limitations of the blockchain, explain their reasons, and sketch possible ways to overcome them. By the end of Step 23, you will understand why the original idea of the blockchain as explained in the previous steps may not be suitable for large-scale commercial applications, what changes were made to overcome these limitations, and how these changes altered the properties of the blockchain.

Stage V: Using the Blockchain, Summary, and Outlook

Steps 24 and 25 consider how the blockchain can be used in real life and what questions should to be addressed when selecting a blockchain application. This stage also points out areas of active research and further development. By the end of Step 25, you will have gained a well-grounded understanding of the blockchain and you will be well prepared to read more advanced texts or to become an active part in the ongoing discussion about the blockchain.

Accompanying Material

The website `www.blockchain-basics.com` offers accompanying material for some of the steps of this book.